

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Inventors: Yasunari KIMURA et al.

Application No.: New Patent Application

Filed: August 2, 2000

For: INDIVIDUAL AUTHENTICATION METHOD, INDIVIDUAL
AUTHENTICATION APPARATUS, ACCOUNTING METHOD,
ACCOUNTING APPARATUS

CLAIM FOR PRIORITY

Assistant Commissioner of Patents
Washington, D.C. 20231

Sir:

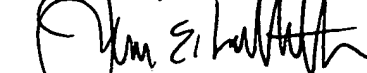
The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified application and the priority provided in 35 USC 119 is hereby claimed:

Japanese Appln. No. 11-219739, Filed August 3, 1999.

In support of this claim, a certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 USC 119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,



James E. Ledbetter

Registration No. 28,732

Date: August 2, 2000

JEL/ldh

Attorney Docket No. JEL 31225

STEVENS DAVIS, MILLER & MOSHER, L.L.P.

1615 L Street, NW, SUITE 850

P.O. BOX 34387

Washington, DC 20043-4387

Telephone: (202) 408-5100; Facsimile: (202) 408-5200

Jc862 U.S. PTO
09/631301
08/02/00

#5

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

JC862 U.S. PTO
09/631301
08/02/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 8月 3日

出 願 番 号

Application Number:

平成11年特許願第219739号

出 願 人

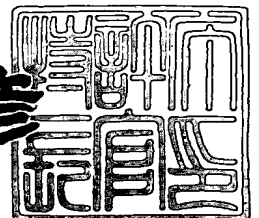
Applicant (s):

松下電器産業株式会社

2000年 3月17日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3017690

【書類名】 特許願

【整理番号】 2931000197

【提出日】 平成11年 8月 3日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/32

【発明者】

【住所又は居所】 神奈川県川崎市多摩区東三田 3 丁目 1 0 番 1 号 松下技
研株式会社内

【氏名】 木村 恭也

【発明者】

【住所又は居所】 神奈川県川崎市多摩区東三田 3 丁目 1 0 番 1 号 松下技
研株式会社内

【氏名】 池田 健

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【プルーフの要否】 不要

【書類名】 明細書

【発明の名称】 個人認証システム

【特許請求の範囲】

【請求項 1】 サービスを提供するサービス提供者が保有するサービス提供装置に、ユーザが接続する場合において、サービス要求を行っているユーザが正規のユーザか否かを認証する個人認証システムであって、

前記サービス提供装置側では、ユーザに関するデータを記憶する会員データベースと、

ユーザが入力する会員IDと、暗証番号等の基本認証パスワード情報に対して、前記会員データベースに記憶されている照合用基本認証パスワード情報を比較照合し、認証を行う基本認証手段と、

前記基本認証手段による認証実行後、会員データベースに登録されているユーザの移動体通信端末呼び出し番号を用いて移動体通信端末へ呼を接続し、呼によって確立した移動体通信通信路を用いて移動体通信経路認証を行う移動体通信経路認証手段と、

前記基本認証手段と前記移動体通信経路認証手段を用いて認証できた場合にサービス提供が可能であると判断する個人認証管理手段を有し、

サービス提供を要求する被認証者側では、前記サービス提供装置と接続されているサービス端末と、前記呼び出し番号を前記会員データベースに登録してある移動体通信端末を有することを特徴とする個人認証システム。

【請求項 2】 移動体通信経路認証手段は、基本認証手段による基本認証実行後、会員データベースに登録されているユーザの移動体通信端末呼び出し番号を用いて移動体通信端末へ呼を接続し、被認証者に対して移動体通信経路認証パスワード情報の要求、及び、被認証者により入力された移動体通信経路認証パスワード情報の入手を行い、前記被認証者により入力された移動体通信経路認証パスワード情報を前記会員データベースに記憶されている照合用移動体通信経路認証パスワード情報と比較照合し、一致した場合を認証成功とすることを特徴とする請求項 1 記載の個人認証システム。

【請求項 3】 サービス要求を行っているサービス端末に会員データベースに

登録してある移動体通信端末を接続し、個人認証することを特徴とする請求項 1 記載の個人認証システム。

【請求項 4】 移動体通信経路認証手段は、基本認証手段による認証実行後、会員データベースに登録されているユーザの移動体通信端末呼び出し番号を用いて移動体通信端末へ呼を接続し、移動体通信端末へテスト信号を発信し、移動体通信端末、サービス端末で前記テスト信号を受信し、発信したテスト信号と受信したテスト信号を比較照合し、一致した場合を認証成功とすることを特徴とする請求項 3 記載の個人認証システム。

【請求項 5】 移動体通信経路認証手段は、基本認証手段による認証実行後、会員データベースに登録されているユーザの移動体通信端末呼び出し番号を用いて移動体通信端末へ呼を接続することにより移動体通信通信路を確立し、サービス端末へテスト信号を発信し、サービス端末、移動体端末、移動体通信通信路と言う経路で前記テスト信号を受信し、発信したテスト信号と受信したテスト信号を照合し、一致した場合を認証成功とすることを特徴とする請求項 3 記載の個人認証システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、電子商取引やパソコン通信等、情報通信を用いてサービスを実現するシステムの個人認証をより確実にする個人認証システムに関するものである。

【 0 0 0 2 】

【従来の技術】

従来より、電子的手段を用いての契約、取り引き等が行われる場合に、その電子的手段を用いようとしている者が正規の契約者であるか否かの認証は、暗証番号、パスワード等によって行われてきた。例えば、パソコン通信の場合であれば、パソコンおよび電話回線を用いてパソコン通信の会員が契約申し込み情報を送信し、パソコン通信事業者側に設置されたサービス提供装置（サービス提供者が保有するサーバをいう）ではこれを受信することで、その両者間の契約を行ってきた。この際、そのパソコン通信会員に成り済まし、不正な利用者が契約を実行

することを排除するための認証手順は次のようなものである。

【0003】

まず、予めパソコンユーザとパソコン通信事業者との間で利用契約を締結する。その際、パソコン通信事業者は正規会員ユーザへ会員ID番号、パスワードを通知する。パソコン通信事業者はパソコン通信を介してユーザからアクセス要求があった時には、アクセス要求しているユーザに対して予め登録させた会員IDおよびパスワードを要求し、ユーザがこれを入力した時にパソコン通信事業者側に記録されている正規会員情報と照合して、これに適合したときには、アクセス要求しているユーザを正規の会員ユーザと認証する。そして、この認証により確立された通信路を用いてアクセス者から送信されてくる、注文情報等は、正規の会員ユーザが送信したものとして受け付けると言うものである。

【0004】

【発明が解決しようとする課題】

しかし、これら従来技術では、以下のような欠点を有していた。

【0005】

従来の個人認証技術では、ハッカーが正規会員ユーザのパソコンの送信ゲート、あるいは、モデム等に侵入し、ここで正規会員ユーザが送信する会員ID番号やパスワードを取得してしまえば、不正利用者による「成り済まし」を排除することは困難である。

【0006】

現在、ハッカーによる会員ID番号およびパスワードの不正取得を防止することを目的に、正規会員ユーザとサービス提供事業者間では、情報の伝達を暗号処理し、通信セキュリティを確保して行われることがある。しかし、パスワード等の不正取得を防止する手段を如何に高度化、複雑化させたところで、より高度な不正取得手段を開発するハッカーに対して従来の個人認証技術は十分安全なものとは言えない。

【0007】

また、予め設定された会員IDおよびパスワードも何らかの手段で他者が知った場合は、本人認証としての役割を果たすことはできない。

【 0 0 0 8 】

本発明は、上記従来技術の課題を解決するもので、不正利用者により正規会員ユーザの会員ID番号およびパスワードの不正取得が行われたとしても不正利用者による「成り済まし」を排除することが可能な確度の高い個人認証システムの提供を目的とする。

【 0 0 0 9 】

【課題を解決するための手段】

この課題を解決するために、本発明は、オープンな情報通信路だけでなく、移動体通信事業者の持つ通信路も用いて個人認証を実行するよう構成したものである。これにより、オープンな情報通信路で不正利用者により正規会員ユーザの会員ID番号およびパスワードの不正取得が行われたとしても不正利用者による「成り済まし」を排除することが可能な確度の高い個人認証システムを実現することができる。

【 0 0 1 0 】

【発明の実施の形態】

本発明の請求項 1 に記載の発明は、サービスを提供するサービス提供者が保有するサーバに、ユーザが接続する場合において、サービス要求を行っているユーザが正規のユーザか否かを認証する個人認証システムであって、前記サーバ側では、ユーザに関するデータを記憶する会員データベースと、ユーザが入力する会員IDと、暗証番号等の基本認証パスワード情報に対して、前記会員データベースに記憶されている照合用基本認証パスワード情報を比較照合し、認証を行う基本認証手段と、前記基本認証手段による認証実行後、会員データベースに登録されているユーザの移動体通信端末呼び出し番号を用いて移動体通信端末へ呼を接続し、呼によって確立した移動体通信通信路を用いて移動体通信経路認証を行う移動体通信経路認証手段と、前記基本認証手段と前記移動体通信経路認証手段を用いて認証できた場合にサービス提供が可能であると判断する個人認証管理手段を有し、サービス提供を要求する被認証者側では、前記サーバと接続されているサービス端末と、前記呼び出し番号を前記会員データベースに登録してある移動体通信端末を有することを特徴とし、オープンな情報通信路で不正利用者により正

規会員ユーザの会員ID番号および基本認証パスワード情報の不正取得が行われたとしても、会員ID番号に対応する移動体通信端末を同時に所有しない限り不正利用者による「成り済まし」の可能性を排除し、且つ、移動体通信端末を携帯する正規会員に対して不正なアクセスがあることを通知するという作用を有する。

【0011】

請求項2に記載の発明は、請求項1記載の発明において、基本認証手段による基本認証実行後、会員データベースに登録されている会員ユーザの移動体通信端末呼び出し番号を用いて移動体通信端末へ呼を接続し、呼によって確立した移動体通信通信路を用いて、被認証者に対して移動体通信経由認証パスワード情報の要求、及び、被認証者により入力された移動体通信経由認証パスワード情報の入手を行い、前記被認証者により入力された移動体通信経由認証パスワード情報を前記会員データベースに記憶されている照合用移動体通信経由認証パスワード情報と比較照合し、一致した場合を認証成功とする移動体通信経由認証手段を特徴としたものであり、オープンな情報通信路で不正利用者により正規会員ユーザの会員ID番号および基本認証手段用パスワード情報の不正取得が行われ、且つ、会員ID番号に対応する移動体通信端末も不正に取得されてしまった場合でも、不正利用者による「成り済まし」の可能性を排除するという作用を有する。

【0012】

請求項3の発明は、請求項1記載の発明において、サービス要求を行っているサービス端末に会員データベースに登録してある移動体通信端末を接続することを特徴としたものであり、オープンな情報通信路で不正利用者により正規会員ユーザの会員ID番号および基本認証手段用パスワード情報の不正取得が行われたとしても、会員ID番号に対応する移動体通信端末を同時に所有しない限り不正利用者による「成り済まし」の可能性を排除するという作用を有する。

【0013】

請求項4の発明は、請求項3記載の発明において、基本認証手段による認証実行後、会員データベースに登録されている会員ユーザの移動体通信端末呼び出し番号を用いて移動体通信端末へ呼を接続し、呼によって確立した移動体通信通信路を用いて、移動体通信端末へテスト信号を発信し、移動体通信端末、サービス

端末、オープンな情報通信路経由で前記テスト信号を受信し、発信したテスト信号と受信したテスト信号を比較し、一致した場合を認証成功とする移動体通信経由認証手段を特徴としたものであり、オープンな情報通信路で不正利用者により正規会員ユーザの会員ID番号および基本認証パスワード情報の不正取得が行われたとしても、会員ID番号に対応する移動体通信端末を同時に所有しない限り不正利用者による「成り済まし」の可能性を排除するという作用を有する。

【0014】

請求項5の発明は、請求項3記載の発明において、基本認証手段による認証実行後、会員データベースに登録されている会員ユーザの移動体通信端末呼び出し番号を用いて移動体通信端末へ呼を接続することにより移動体通信通信路を確立し、サービス端末へオープンな情報通信路を用いてテスト信号を発信し、サービス端末、移動体端末、移動体通信通信路経由で前記テスト信号を受信し、発信したテスト信号と受信したテスト信号を比較し、一致した場合を認証成功とする移動体通信経由認証手段を特徴としたものであり、オープンな情報通信路で不正利用者により正規会員ユーザの会員ID番号および基本認証パスワード情報の不正取得が行われたとしても、会員ID番号に対応する移動体通信端末を同時に所有しない限り不正利用者による「成り済まし」の可能性を排除するという作用を有する。

【0015】

以下、本発明について、図面を参照しながら説明する。

【0016】

(実施の形態1)

図1は本実施の形態における個人認証システムを示す概念図である。図1において、300は、オープンな情報通信路を用いてサービスを提供するサービス提供者が保有するサービス提供装置、100は、認証対象である被認証者、101は、サービス提供装置300から被認証者100へのサービス提供を実現するサービス端末、102は、被認証者100が所持するサービス提供装置300に事前登録されている移動体通信端末、400は、移動体通信端末102を統括するPHS、携帯電話等の移動体通信事業者、202は、サービス端末101とサービ

ス提供装置 300 を接続し、サービス提供装置 300 からサービス端末 101 へサービスを供給するオープンな情報通信路、201 は、移動体通信事業者 400 と移動体通信端末 102 を接続する移動体通信通信路である。

【0017】

ここで、オープンな情報通信路 202 とはインターネットなど不特定多数のユーザが任意のサービス提供者へアクセス可能な情報通信路を示しており、このオープンな情報通信路 202 を用いてサービス提供装置 300 は、例えば、パソコン通信プロバイダサービス、電子商取引サービス等を提供する。

【0018】

なお、図 1 においては、サービス利用者である被認証者 100 が一人のみ示されているが、一般的応用においては複数の被認証者および複数のサービス端末が存在しており、被認証者 100 はその内の一人を示すことになる。

【0019】

図 2 は、本実施の形態におけるサービス提供装置 300 の構成を示す概念図である。図 2 において、310 は、サービス対象者として事前登録されている会員の会員ユーザ情報を記憶する会員データベース、320 は、サービス要求を行っているユーザが正規の会員ユーザか否かを認証、判断する個人認証部である。また、個人認証部は、オープンな情報通信路 202 を用いて会員であることを認証する基本認証手段 321 と、正規会員の所持している移動体通信端末を用いて会員であることを認証する移動体通信経由認証手段 322 と、基本認証手段 321 および移動体通信経由認証手段 322 を統括管理し、個人認証の判断を行う個人認証管理手段から構成されている。

【0020】

図 3 は、本実施の形態で示す個人認証システムを実現するために必要な会員ユーザ情報の例を示しており、この会員ユーザ情報は、会員データベース 310 に事前に登録されている。

【0021】

図 3 には、3名の会員ユーザ情報が記憶されている例を示しており、会員情報の内訳は、「会員氏名」、及び、オープンな情報通信路 202 経由で認証を行う

時に用いる「会員ID番号」、「基本認証パスワード情報」と移動体通信通信路 201 経由で認証を行う時に用いる「移動体通信端末呼び出し番号」、「移動体通信経由認証パスワード情報」である。

【0022】

図4は、本実施の形態で示す個人認証システムの認証手順を示したコラボレーション図であり、手順1～手順25の数字は、認証手順の順番を示している。以下、本実施の形態で示す個人認証システムの動作を図4の認証順番毎に説明する。

【0023】

＜手順1＞

被認証者100は、図1に示すサービス提供者の保有するサービス提供装置300のサービス提供を受けるために、サービス端末101に、「会員ID番号」及び「基本認証パスワード情報」を入力する。ここで、「会員ID番号」及び「基本認証パスワード情報」とは、被認証者100がサービス提供者とサービス提供契約を交わした際に、サービス提供者から通知されるものであり、通知された前記「会員ID番号」及び「基本認証パスワード情報」は、サービス提供者が保有するサービス提供装置300内の会員データベース310に被認証者100の氏名および被認証者100の所持する移動体通信端末102の移動体端末呼び出し番号と対応付けられ記憶されているものとする。

【0024】

＜手順2＞

「会員ID番号」及び「基本認証パスワード情報」を入力されたサービス端末101はオープンな情報通信路202を経由して前記「会員ID番号」及び「ユーザ入力基本認証パスワード情報」をサービス提供装置300内の個人認証管理手段へ送信し、サービス提供資格審査としての個人認証を要求する。

【0025】

ここで、オープンな情報通信路202を使用して前記「会員ID番号」及び「ユーザ入力基本認証パスワード情報」を通信する場合、これら情報の不正取得を防止することを目的にサービス端末101とサービス提供装置300間では情報の

伝達を暗号処理し、通信セキュリティを確保してもよい。また、「ユーザ入力基本認証パスワード情報」とは、ユーザがユーザ端末101から入力した「基本認証パスワード情報」を示す。

【0026】

〈手順3〉

個人認証要求および「会員ID番号」「ユーザ入力基本認証パスワード情報」を受信した個人認証管理手段323は、「会員ID番号」「ユーザ入力基本認証パスワード情報」を基本認証手段321に送付し、「会員ID番号」に対応するサービス対象者の個人認証を要求する。

【0027】

〈手順4〉

「会員ID番号」「ユーザ入力基本認証パスワード情報」を個人認証管理手段323から受け取った基本認証手段321は、会員データベース310に対して、個人認証管理手段323より受け取った「会員ID番号」に対応する「照合用基本認証パスワード情報」を要求する。

【0028】

ここで、「照合用基本認証パスワード情報」とは、会員データベース310が、記憶している「会員ID番号」に対応した「基本認証パスワード情報」を示している。

【0029】

〈手順5〉

会員データベース310は、要求のあった「会員ID番号」をキーワードに、データベース内の会員ユーザ情報の検索を実行し、同一の「会員ID番号」を発見した場合には、この「会員ID番号」に対応する「照合用基本認証パスワード情報」を基本認証手段321へ送付する。

【0030】

ここで、検索の結果、要求のあった「会員ID番号」が発見できなかった場合は、会員データベース310は、基本認証手段321へ会員ID番号がないことを通知する。

【0031】

＜手順6＞

基本認証手段321は、会員データベース310から「照合用基本認証パスワード情報」が返送されてくると、前記「照合用基本認証パスワード情報」と「ユーザ入力基本認証パスワード情報」を比較照合し、同一であれば、基本認証が成立したと判定し、同一でない場合は、基本認証が不成立であったと判定する。

【0032】

ここで、会員データベース310から検索すべき「会員ID番号」が存在しない旨の通知を受けた場合、基本認証手段321は、基本認証が不成立であったと判定する。

【0033】

＜手順7＞

基本認証手段321は、「会員ID番号」と共に、基本認証の判定結果を個人認証管理手段323へ通知する。

【0034】

＜手順8＞

個人認証管理手段323は、基本認証手段321から送られてきた認証結果が、基本認証成立である場合には、「会員ID番号」を移動体通信経路認証手段322へ送付し、移動体通信経路認証を要求する。

【0035】

ここで、基本認証手段321から送られてきた基本認証の結果が、基本認証不成立であった場合、個人認証管理手段323はサービス端末101へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【0036】

＜手順9＞

「会員ID番号」を個人認証管理手段323から受け取った移動体通信経路認証手段322は、会員データベース310に対して、個人認証管理手段323より受け取った「会員ID番号」に対応する「照合用移動体通信経路認証パスワード情報」および「移動体通信端末呼び出し番号」を要求する。

【0037】

ここで、「照合用移動体通信経路認証パスワード情報」とは、会員データベース310が、記憶している「会員ID番号」に対応した「移動体通信経路認証パスワード情報」を示している。

【0038】

＜手順10＞

会員データベース310は、要求のあった「会員ID番号」をキーワードに、データベース内の会員ユーザ情報の検索を実行し、同一の「会員ID番号」を発見した場合には、この「会員ID番号」に対応する「照合用移動体通信経路認証パスワード情報」および「移動体通信端末呼び出し番号」を移動体通信経路認証手段322へ送付する。

【0039】

なお、検索の結果、要求のあった「会員ID番号」が発見できなかった場合は、会員データベース310は、移動体通信認証手段322へ会員ID番号が存在しないことを通知する。

【0040】

＜手順11＞

移動体通信経路認証手段322は、会員データベース310から「照合用移動体通信経路認証パスワード情報」および「移動体通信端末呼び出し番号」が返送されてくると、移動体通信事業者400に対して「移動体通信端末呼び出し番号」を使用して移動体通信端末102への回線接続要求を行う。なお、移動体通信経路認証手段322が、会員データベース310から検索すべき「会員ID番号」が存在しない旨の通知を受けた場合、移動体通信手段322は、基本認証が不成立であったと判定し、手順24へ手続きを進める。

【0041】

また、移動体通信経路認証手段322から移動体通信事業者400へ回線接続要求を送信する際使用する通信路は、専用回線あるいは、電話通信網等の公共回線のどちらを使用しても良い。

【0042】

〈手順 12〉～〈手順 15〉

手順 12、手順 13、手順 14、手順 15 の操作は、移動体通信事業者 400 の回線接続方法により異なるが、以下、携帯電話等の一般的回線接続方法を示す。

【0043】

〈手順 12〉

移動体通信事業者 400 は、移動体通信通信路 201 を用いて移動体通信端末 102 に対して回線接続要求を行う。ここで、移動体通信端末 102 が他の通信に使用されている等で回線接続が不可能である場合は、移動体通信事業者 400 は、回線接続失敗と判定し、手順 16 へ進む。

【0044】

〈手順 13〉

移動体通信事業者 400 から回線接続要求を受けた移動体通信端末 102 は、回線接続要求を受けていることを被認証者 100 に呼び出しベル、バイブレータ等を用いて通知する。

【0045】

〈手順 14〉

被認証者 100 は、移動体通信端末 102 に設置されている応答ボタン等を押すことにより回線接続要求に応答する。

【0046】

〈手順 15〉

移動体通信端末 102 は、被認証者 100 から応答があったことを移動体通信通信路 201 を用いて移動体通信事業者 400 へ通知し、移動体通信通信路 201 に回線を設定する。

【0047】

〈手順 16〉

移動体通信事業者 400 は、回線接続結果を移動体通信経由認証手段 322 へ通知する。ここで、移動体通信経由認証手段 322 は、移動体通信事業者 400 から送付された回線接続結果が、回線接続失敗であった場合、移動体通信経由認

証が不成立であったと判定し、手順 24 へ進む。

【0048】

〈手順 17〉～〈手順 19〉

移動体通信事業者 400 からの回線接続結果が回線接続成功であった場合、移動体通信経路認証手段 322 は、移動体通信通信路 201 に設定された回線を用いて「移動体通信経路認証パスワード情報」の入力を被認証者 100 へ要求する。

【0049】

ここで、「移動体通信経路認証パスワード情報」とは、被認証者 100 がサービス提供者とサービス提供契約を交わした際に、サービス提供者から通知されるものであり、通知された前記「移動体通信経路認証パスワード情報」は、サービス提供者が保有するサービス提供装置 300 内の会員データベース 310 に被認証者 100 の氏名および被認証者 100 の所持する移動体通信端末 102 の移動体端末呼び出し番号と対応付けられ記憶されているものとする。

【0050】

なお、サービス提供契約を交わした正規の会員ユーザ以外の不正利用者が、何らかの方法で正規会員ユーザの「基本認証パスワード情報」および「会員ID番号」を入手し、正規会員ユーザに成り済まし、サービス提供要求をした場合、正規会員ユーザは、前記「移動体通信経路認証パスワード情報」の入力要求を移動体通信端末 102 から受けることにより、不正利用の要求が行われていることを知る ことができる。

【0051】

〈手順 20〉～〈手順 22〉

被認証者 100 が、「移動体通信経路認証パスワード情報」を移動体通信端末 102 へ入力すると、移動体通信端末 102 は、移動体通信通信路 201 に設定された回線を用いて「ユーザ入力移動体通信経路認証パスワード情報」を移動体通信経路認証手段 322 へ送付する。ここで、「ユーザ入力移動体通信経路認証パスワード情報」とは、ユーザが移動体通信端末 102 から入力した「移動体通信経路認証パスワード情報」を示す。

【0052】

＜手順23＞

移動体通信経路認証手段322は、「ユーザ入力移動体通信経路認証パスワード情報」が返送されてくると、前記「照合用移動体通信経路認証パスワード情報」と「ユーザ入力移動体通信経路認証パスワード情報」を比較照合し、同一であれば、移動体通信経路認証が成立したと判定し、同一でない場合は、移動体通信経路認証が不成立であったと判定する。

【0053】

＜手順24＞

移動体通信経路認証手段322は、「会員ID番号」と共に、移動体通信経路認証の認証結果を個人認証管理手段323へ通知する。

【0054】

＜手順25＞

個人認証管理手段323は、移動体通信経路認証手段322から送られてきた認証結果が、移動体通信経路認証の成立である場合には、個人認証が成功したと判定し、サービス提供装置300からサービス端末101へのサービス提供を開始する。

【0055】

また、認証結果が、移動体通信経路認証が不成立であった場合、個人認証管理手段323はサービス端末101へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【0056】

(実施の形態2)

図5は本実施の形態における個人認証システムを示す概念図である。図5において、被認証者100、移動体通信通信路201、オープンな情報通信路202、サービス提供装置300、移動体通信事業者400は、図1に示す実施形態1の個人認証システムと同様の機能を有しており、本実施の形態と実施形態1の個人認証システムとの差異は、本実施の形態で示す個人認証システムでは、個人認証を実施する際、情報通信端末101と移動体通信端末102間を「サービス端

末、移動体通信端末間通信路」203を用いて接続する点であり、サービス端末101は、実施の形態1の機能に加え「サービス端末、移動体通信端末間通信路」203とのインターフェース機能、および移動体通信端末102の呼び出しに対して応答する機能が付加されている。

【0057】

また、移動体通信端末102も実施の形態1の機能に加え「サービス端末、移動体通信端末間通信路」203とのインターフェース機能を付加されている。ここで、「サービス端末、移動体通信端末間通信路」203とは、有線を用いた接続、無線を用いた接続、あるいは、音響カプラ等を用いた接続路を示す。

【0058】

図6は、本実施の形態で示す個人認証システムを実現するために必要な会員ユーザ情報の例を示しており、この会員ユーザ情報は、図2に示す会員データベース310に事前に登録されている。

【0059】

図6には、3名の会員ユーザ情報が記憶されている例を示しており、会員情報の内訳は、「会員氏名」、及び、オープンな情報通信路202経由で認証を行う時に用いる「会員ID番号」、「基本認証パスワード情報」と移動体通信通信路経由で認証を行う時に用いる「移動体通信端末呼び出し番号」である。

【0060】

図7は、本実施の形態で示す個人認証システムの認証手順を示したコラボレーション図であり、手順1～手順24の数字は、認証手順の順番を示している。以下、本実施の形態で示す個人認証システムの動作を図7の認証順番毎に説明する。

【0061】

<手順1>

被認証者100は、所持する移動体通信端末102をサービス端末101へ「サービス端末、移動体通信端末間通信路」を用いて接続する。

【0062】

<手順2>～<手順9>

被認証者 100 のサービス提供要求から基本認証の成立までは、図 4 の実施の形態 1 の個人認証手順<手順 1>～<手順 8>と同様である。

【0063】

<手順 10>

「会員ID番号」を個人認証管理手段 323 から受け取った移動体通信経路認証手段 322 は、会員データベース 310 に対して、個人認証管理手段 323 より受け取った「会員ID番号」に対応する「移動体通信端末呼び出し番号」を要求する。

【0064】

<手順 11>

会員データベース 310 は、要求のあった「会員ID番号」をキーワードに、データベース内の会員ユーザ情報の検索を実行し、同一の「会員ID番号」を発見した場合には、この「会員ID番号」に対応する「移動体通信端末呼び出し番号」を移動体通信経路認証手段 322 へ送付する。

【0065】

なお、検索の結果、要求のあった「会員ID番号」が発見できなかった場合は、会員データベース 310 は、移動体通信認証手段 322 へ会員ID番号が存在しないことを通知する。

【0066】

<手順 12>

移動体通信経路認証手段 322 は、会員データベース 310 から「移動体通信端末呼び出し番号」が返送されてくると、移動体通信事業者 400 に対して「移動体通信端末呼び出し番号」を使用して移動体通信端末 102 への回線接続要求を行う。なお、移動体通信経路認証手段 322 が、会員データベース 310 から検索すべき「会員ID番号」が存在しない旨の通知を受けた場合、移動体通信手段 322 は、基本認証が不成立であったと判定し、手順 23 へ手続きを進める。

【0067】

また、移動体通信経路認証手段 322 から移動体通信事業者 400 へ回線接続要求を送信する際使用する通信路は、専用回線あるいは、電話通信網等の公共回

線のどちらを使用しても良い。

【0068】

＜手順13＞

移動体通信事業者400は、移動体通信通信路201を用いて移動体通信端末102に対して回線接続要求を行う。ここで、移動体端末102が他の通信に使用されている等で回線接続が不可能である場合は、移動体通信事業者400は、回線接続失敗と判定し、手順17へ進む。

【0069】

＜手順14＞

移動体通信事業者400から回線接続要求を受けた移動体通信端末102は、回線接続要求を受けていることをサービス端末101へ「サービス端末、移動体通信端末間通信路」203を用いて通知する。

【0070】

＜手順15＞

サービス端末101は、「サービス端末、移動体通信端末間通信路」203を用いて移動体通信端末102に回線接続要求に対する応答を通知する。

【0071】

＜手順16＞

移動体通信端末102は、サービス端末101から応答があったことを移動体通信通信路201を用いて移動体通信事業者400へ通知し、移動体通信通信路201に回線を設定する。

【0072】

＜手順17＞

移動体通信事業者400は、回線接続結果を移動体通信経路認証手段322へ通知する。ここで、移動体通信経路認証手段322は、移動体通信事業者400から送付された回線接続結果が、回線接続失敗であった場合、移動体通信経路認証が不成立であったと判定し、手順23へ進む。

【0073】

＜手順18＞

移動体通信事業者 400 からの回線接続結果が回線接続成功であった場合、移動体通信経路認証手段 322 は、テスト信号を移動体通信事業者 400 へ送信し、送信したテスト信号を送信テスト信号として記憶する。

【0074】

ここで、テスト信号は、乱数等を用いて発生させた任意の信号を用いてもよいし、事前に移動体通信経路認証手段 322 が記憶している任意の信号を用いてもよい。

【0075】

<手順 19>

移動体通信事業者 400 は、移動体通信通信路 201 に設定された回線を用いて前記テスト信号を移動体通信端末 102 へ送信する。

【0076】

<手順 20>

移動体通信端末 102 は、「サービス端末、移動体通信端末間通信路」203 を用いて前記テスト信号をサービス端末 101 へ送信する。

【0077】

<手順 21>

サービス端末 101 は、オープンな情報通信路 202 を用いて前記テスト信号を移動体通信経路認証手段 322 へ送信する。

【0078】

<手順 22>

移動体通信経路認証手段 322 は、前記テスト信号を受信すると、記憶している「送信テスト信号」と受信したテスト信号を比較照合し、同一であれば、移動体通信経路認証が成立したと判定し、同一でない場合は、移動体通信認証経路認証が不成立であったと判定する。

【0079】

<手順 23>

移動体通信経路認証手段 322 は、「会員 ID 番号」と共に、移動体通信経路認証の認証結果を個人認証管理手段 323 へ通知する。

【0080】

<手順24>

個人認証管理手段323は、移動体通信経路認証手段322から送られてきた認証結果が、移動体通信経路認証の成立である場合には、個人認証が成功したと判定し、サービス提供装置300からサービス端末101へのサービス提供を開始する。

【0081】

また、認証結果が、移動体通信経路認証が不成立であった場合、個人認証管理手段323はサービス端末101へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【0082】

(実施の形態3)

本実施の形態の構成は、図5に示す実施の形態2の個人認証システムと同様である。また、本実施の形態で示す個人認証システムを実現するために必要な会員ユーザ情報も図6に示す実施の形態2の会員情報と同様である。

【0083】

本実施の形態と実施の形態2では、認証手順が異なっており、図8は、本実施の形態で示す個人認証システムの認証手順を示したコラボレーション図である。ここで、図9の手順1～手順24の数字は、認証手順の順番を示している。以下、本実施の形態で示す個人認証システムの動作を図8の認証順番毎に説明する。

【0084】

<手順1>～<手順17>

サービス端末101と移動体通信端末102の接続、被認証者100の基本認証成立、および、移動体通信通信路201上での移動体通信端末101と移動体通信経路認証手段322間の回線設定までの手順は、図7の実施の形態2の個人認証手順<手順1>～<手順17>と同様である。

【0085】

<手順18>

移動体通信事業者400からの回線接続結果が回線接続成功であった場合、移

動体通信経由認証手段 322 は、テスト信号をオープンな情報通信路 202 を用いてサービス端末 101 へ送信し、送信したテスト信号を送信テスト信号として記憶する。

【0086】

ここで、テスト信号は、乱数等を用いて発生させた任意の信号を用いてもよいし、事前に移動体通信経由認証手段 322 が記憶している任意の信号を用いてもよい。

【0087】

〈手順 19〉

サービス端末 101 は、「サービス端末、移動体通信端末間通信路」203 を用いて前記テスト信号を移動体通信端末 102 へ送信する。

【0088】

〈手順 20〉

移動体通信端末 102 は、移動体通信通信路 201 に設定された回線を用いて前記テスト信号を移動体通信事業者 400 へ送信する。

【0089】

〈手順 21〉

移動体通信事業者 400 は、前記テスト信号を移動体通信経由認証手段 322 へ送信する。

【0090】

〈手順 22〉

移動体通信経由認証手段 322 は、前記テスト信号を受信すると、記憶している「送信テスト信号」と受信したテスト信号を比較照合し、同一であれば、移動体通信経由認証が成立したと判定し、同一でない場合は、移動体通信認証経由認証が不成立であったと判定する。

【0091】

〈手順 23〉

移動体通信経由認証手段 322 は、「会員ID番号」と共に、移動体通信経由認証の認証結果を個人認証管理手段 323 へ通知する。

【0092】

＜手順24＞

個人認証管理手段323は、移動体通信経由認証手段322から送られてきた認証結果が、移動体通信経由認証の成立である場合には、個人認証が成功したと判定し、サービス提供装置300からサービス端末101へのサービス提供を開始する。

【0093】

また、認証結果が、移動体通信経由認証が不成立であった場合、個人認証管理手段323はサービス端末101へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【0094】

（実施の形態4）

本実施の形態の構成は、図5に示す実施の形態2の個人認証システムと同様である。また、本実施の形態で示す個人認証システムを実現するために必要な会員ユーザ情報も図6に示す実施の形態2の会員情報と同様である。本実施の形態と実施の形態2では、認証手順が異なっており、図9は、本実施の形態で示す個人認証システムの認証手順を示したコラボレーション図である。

【0095】

ここで、図9の手順1～手順24の数字は、認証手順の順番を示している。以下、本実施の形態で示す個人認証システムの動作を図9の認証順番毎に説明する。

【0096】

＜手順1＞～＜手順12＞

被認証者100のサービス提供要求から基本認証の成立、移動体通信端末102の呼び出し操作までは、図7の実施の形態2の個人認証手順＜手順2＞～＜手順13＞と同様である。

【0097】

＜手順13＞

移動体通信事業者400から回線接続要求を受けた移動体通信端末102は、

回線接続要求を受けていることを被認証者 100 に呼び出しベル、パイプレータ等を用いて通知する。

【0098】

〈手順 14〉

被認証者 100 は、所持する移動体通信端末 102 をサービス端末 101 へ「サービス端末、移動体通信端末間通信路」203 を用いて接続する。

【0099】

〈手順 15〉

被認証者 100 は、移動体通信端末 102 に設置されている応答ボタン等を押すことにより回線接続要求に応答する。なお、この応答作業は、手順 14 の移動体通信端末 102 とサービス端末 101 の接続作業により自動的に実施されることとしてもよい。

【0100】

〈手順 16〉

移動体通信端末 102 は、応答があったことを移動体通信通信路 201 を用いて移動体通信事業者 400 へ通知し、移動体通信通信路 201 に回線を設定する。

【0101】

〈手順 17〉

移動体通信事業者 400 は、回線接続結果を移動体通信経路認証手段 322 へ通知する。ここで、移動体通信経路認証手段 322 は、移動体通信事業者 400 から送付された回線接続結果が、回線接続失敗であった場合、移動体通信経路認証が不成立であったと判定し、手順 23 へ進む。

【0102】

〈手順 18〉

移動体通信事業者 400 からの回線接続結果が回線接続成功であった場合、移動体通信経路認証手段 322 は、テスト信号を移動体通信事業者 400 へ送信し、送信したテスト信号を送信テスト信号として記憶する。ここで、テスト信号は、乱数等を用いて発生させた任意の信号を用いてもよいし、事前に移動体通信経

由認証手段 322 が記憶している任意の信号を用いてもよい。

【0103】

〈手順 19〉

移動体通信事業者 400 は、移動体通信通信路 201 に設定された回線を用いて前記テスト信号を移動体通信端末 102 へ送信する。

【0104】

〈手順 20〉

移動体通信端末 102 は、「サービス端末、移動体通信端末間通信路」 203 を用いて前記テスト信号をサービス端末 101 へ送信する。

【0105】

〈手順 21〉

サービス端末 101 は、オープンな情報通信路 202 を用いて前記テスト信号を移動体通信経由認証手段 322 へ送信する。

【0106】

〈手順 22〉

移動体通信経由認証手段 322 は、前記テスト信号を受信すると、記憶している「送信テスト信号」と受信したテスト信号を比較照合し、同一であれば、移動体通信経由認証が成立したと判定し、同一でない場合は、移動体通信認証経由認証が不成立であったと判定する。

【0107】

〈手順 23〉

移動体通信経由認証手段 322 は、「会員 ID 番号」と共に、移動体通信経由認証の認証結果を個人認証管理手段 323 へ通知する。

【0108】

〈手順 24〉

個人認証管理手段 323 は、移動体通信経由認証手段 322 から送られてきた認証結果が、移動体通信経由認証の成立である場合には、個人認証が成功したと判定し、サービス提供装置 300 からサービス端末 101 へのサービス提供を開始する。

【0109】

また、認証結果が、移動体通信経路認証が不成立であった場合、個人認証管理手段323はサービス端末101へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【0110】

(実施の形態5)

本実施の形態の構成は、図5に示す実施の形態2の個人認証システムと同様である。また、本実施の形態で示す個人認証システムを実現するために必要な会員ユーザ情報も図6に示す実施の形態2の会員情報と同様である。本実施の形態と実施の形態2では、認証手順が異なっており、図10は、本実施の形態で示す個人認証システムの認証手順を示したコラボレーション図である。

【0111】

ここで、図10の手順1～手順24の数字は、認証手順の順番を示している。以下、本実施の形態で示す個人認証システムの動作を図10の認証順番毎に説明する。

【0112】

<手順1>～<手順17>

被認証者100のサービス提供要求から基本認証の成立、移動体通信通信路201上での移動体通信端末101と移動体通信経路認証手段322間の回線設定までの手順は、図9の実施の形態4の個人認証手順<手順1>～<手順17>と同様である。

【0113】

<手順18>

移動体通信事業者400からの回線接続結果が回線接続成功であった場合、移動体通信経路認証手段322は、テスト信号をオープンな情報通信路202を用いてサービス端末101へ送信し、送信したテスト信号を送信テスト信号として記憶する。

【0114】

ここで、テスト信号は、乱数等を用いて発生させた任意の信号を用いてもよい

し、事前に移動体通信経路認証手段 322 が記憶している任意の信号を用いてもよい。

【0115】

〈手順 19〉

サービス端末 101 は、「サービス端末、移動体通信端末間通信路」203 を用いて前記テスト信号を移動体通信端末 102 へ送信する。

【0116】

〈手順 20〉

移動体通信端末 102 は、移動体通信通信路 201 に設定された回線を用いて前記テスト信号を移動体通信事業者 400 へ送信する。

【0117】

〈手順 21〉

移動体通信事業者 400 は、前記テスト信号を移動体通信経路認証手段 322 へ送信する。

【0118】

〈手順 22〉

移動体通信経路認証手段 322 は、前記テスト信号を受信すると、記憶している「送信テスト信号」と受信したテスト信号を比較照合し、同一であれば、移動体通信経路認証が成立したと判定し、同一でない場合は、移動体通信認証経路認証が不成立であったと判定する。

【0119】

〈手順 23〉

移動体通信経路認証手段 322 は、「会員 ID 番号」と共に、移動体通信経路認証の認証結果を個人認証管理手段 323 へ通知する。

【0120】

〈手順 24〉

個人認証管理手段 323 は、移動体通信経路認証手段 322 から送られてきた認証結果が、移動体通信経路認証の成立である場合には、個人認証が成功したと判定し、サービス提供装置 300 からサービス端末 101 へのサービス提供を開

始する。

【0121】

また、認証結果が、移動体通信経路認証が不成立であった場合、個人認証管理手段323はサービス端末101へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【0122】

【発明の効果】

オープンな情報通信路で不正利用者により正規会員ユーザの会員ID番号および基本認証パスワード情報の不正取得が行われたとしても、会員ID番号に対応する移動体通信端末を同時に所有しない限り不正利用者による「成り済まし」の可能性を排除し、且つ、移動体通信端末を携帯する正規会員に対して不正なアクセスがあることを通知することができる。

【図面の簡単な説明】

【図1】

本発明の第1実施形態の個人認証システムを示す概念図

【図2】

本発明の第1実施形態、第2実施形態、第3実施形態、第4実施形態および第5実施形態の個人認証システムにおけるサービス提供装置の構成を示す概念図

【図3】

本発明の第1実施形態の個人認証システムを実現するために必要な会員ユーザ情報の例を示す図

【図4】

本発明の第1実施形態の個人認証システムの認証手順を示したコラボレーション図

【図5】

本発明の第2実施形態、第3実施形態、第4実施形態および第5実施形態の個人認証システムを示す概念図

【図6】

本発明の第2実施形態、第3実施形態、第4実施形態および第5実施形態の個

人認証システムを実現するために必要な会員ユーザ情報の例を示す図

【図 7】

本発明の第 2 実施形態の個人認証システムの認証手順を示したコラボレーション図

【図 8】

本発明の第 3 実施形態の個人認証システムの認証手順を示したコラボレーション図

【図 9】

本発明の第 4 実施形態の個人認証システムの認証手順を示したコラボレーション図

【図 1 0】

本発明の第 5 実施形態の個人認証システムの認証手順を示したコラボレーション図

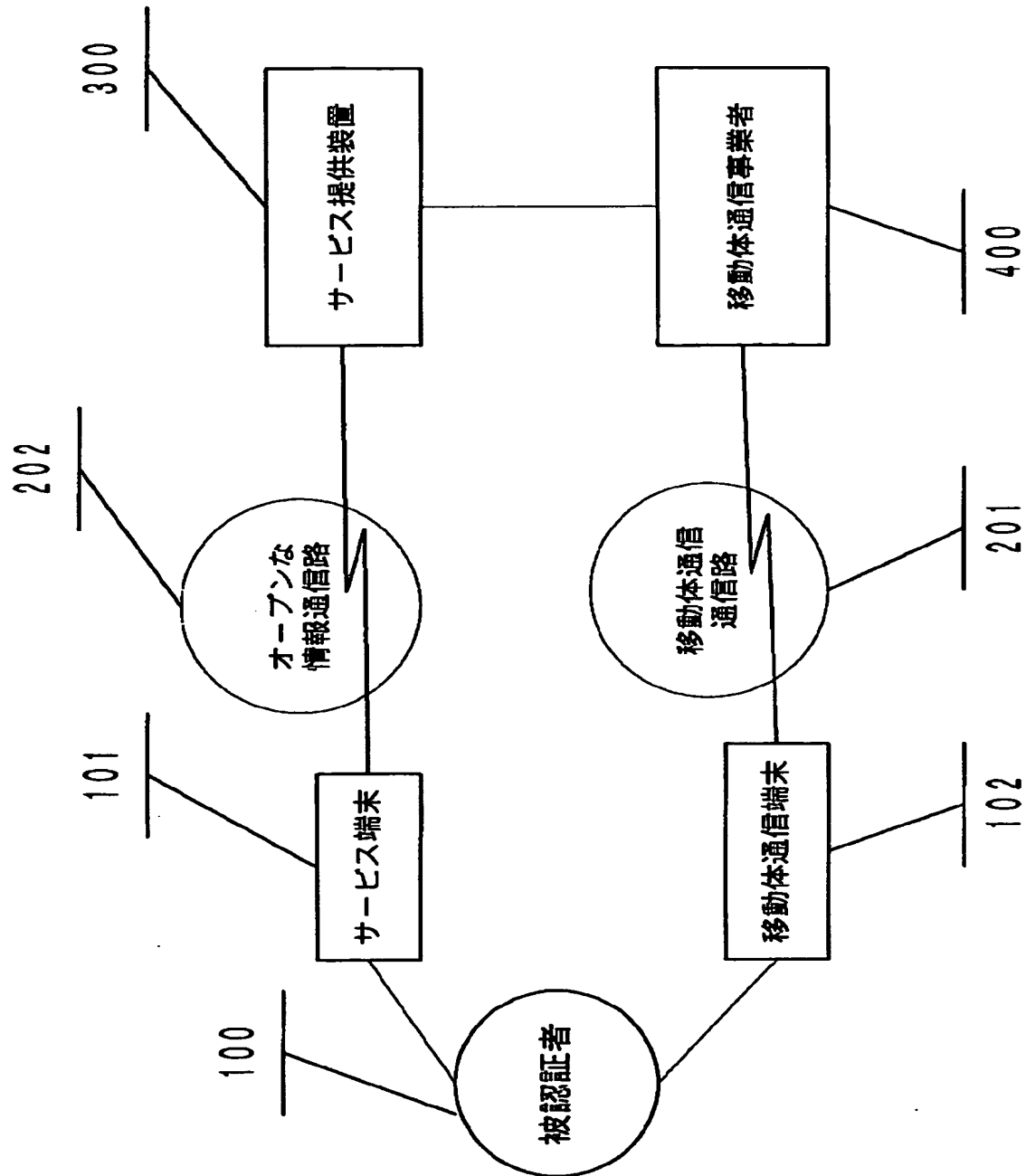
【符号の説明】

- 1 0 0 被認証者
- 1 0 1 サービス端末
- 1 0 2 移動体通信端末
- 2 0 1 移動体通信通信路
- 2 0 2 オープンな情報通信路
- 2 0 3 サービス端末、移動体通信端末間通信路
- 3 0 0 サービス提供装置
- 3 1 0 会員データベース
- 3 2 0 個人認証部
- 3 2 1 基本認証手段
- 3 2 2 移動体通信経路認証手段
- 3 2 3 個人認証管理手段
- 4 0 0 移動体通信事業者

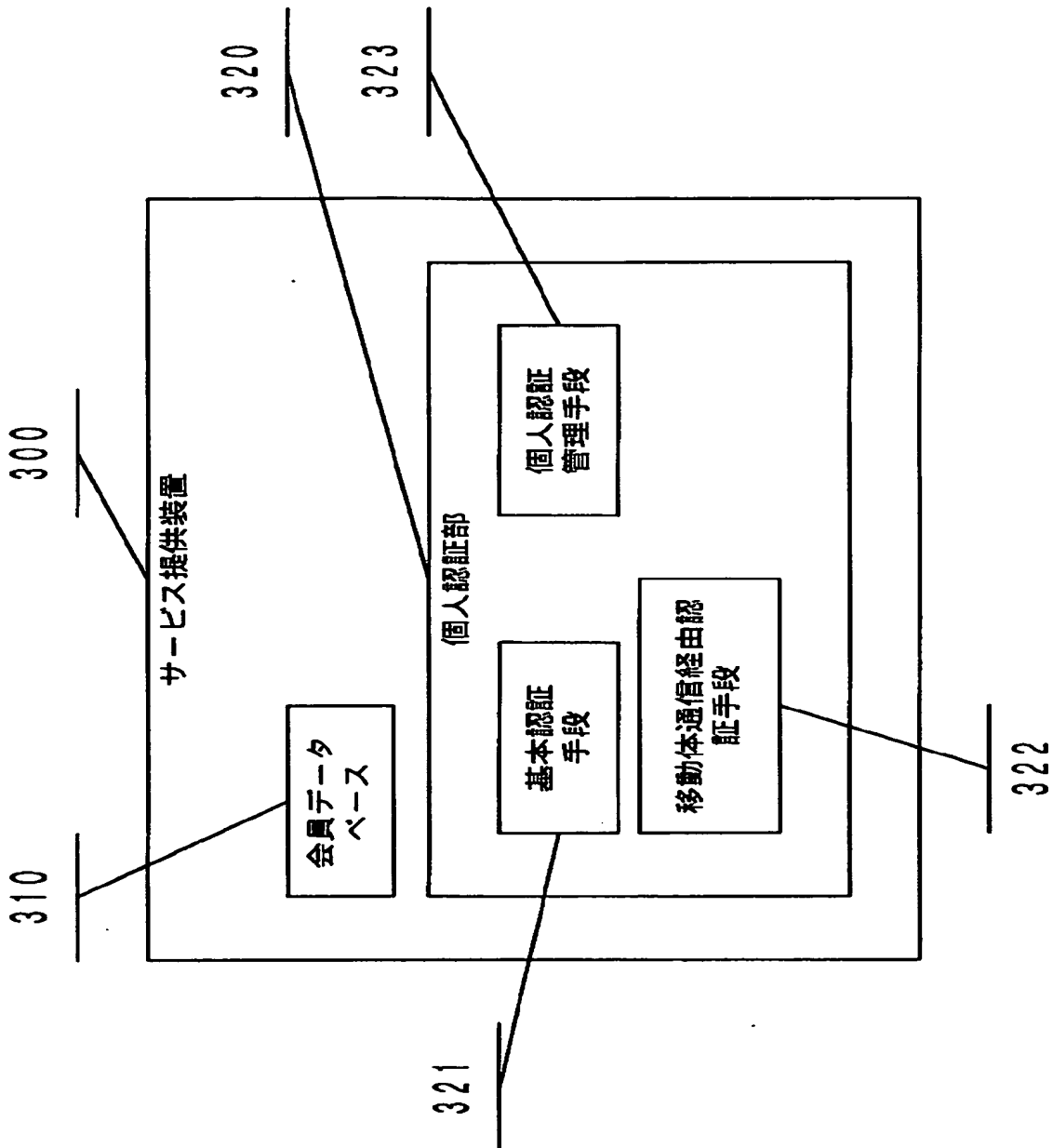
【書類名】

図面

【図 1】



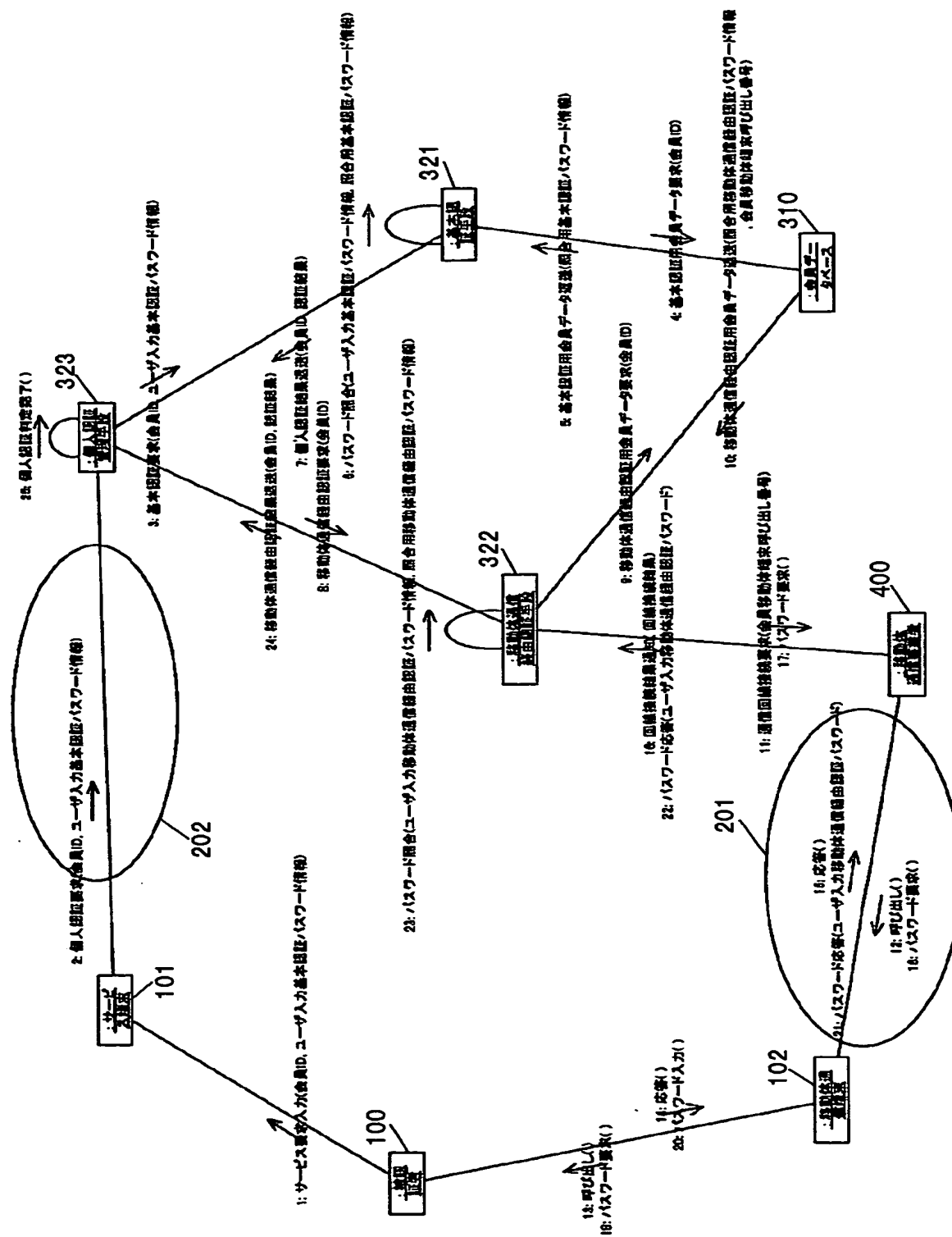
【図 2】



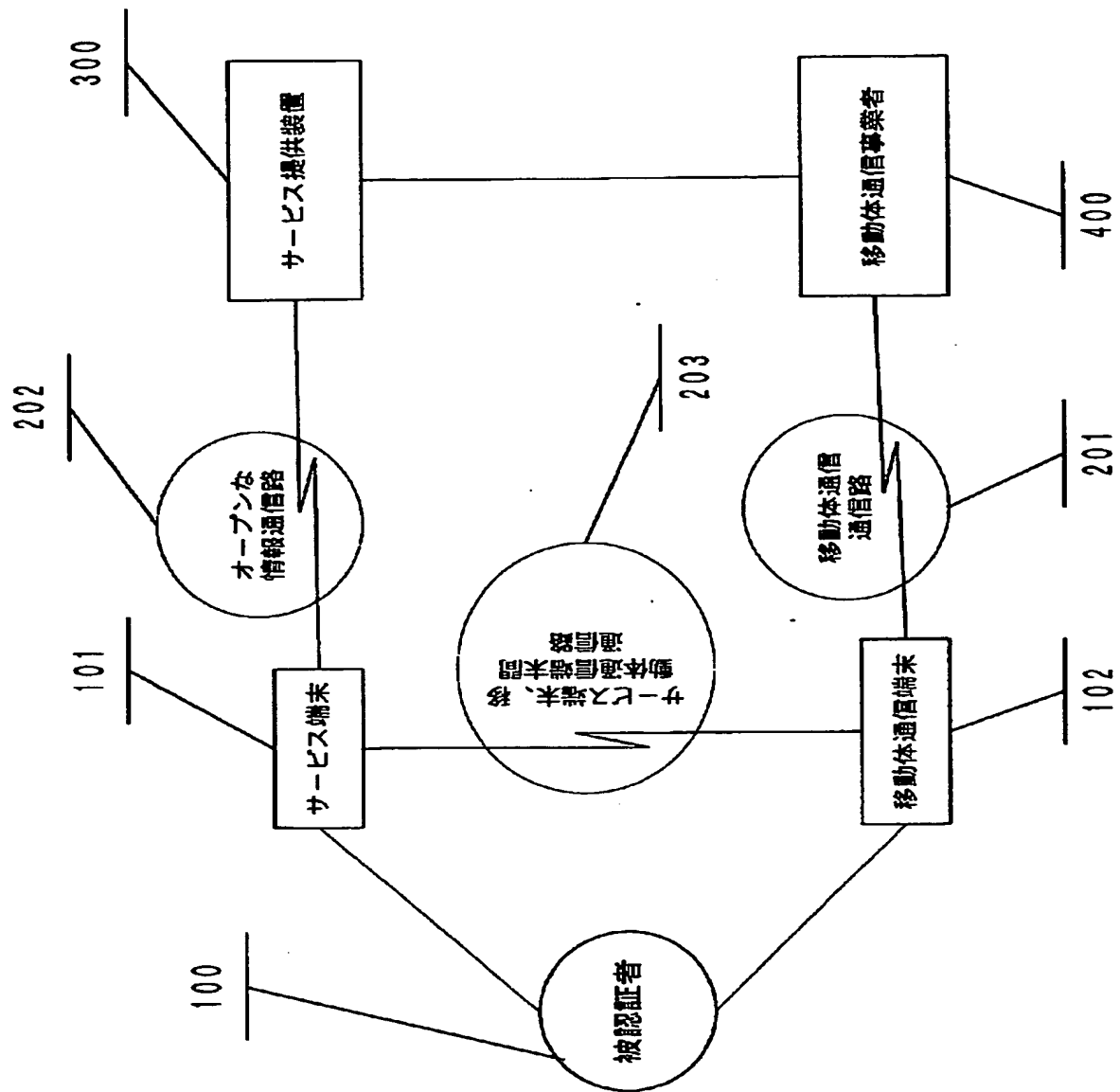
【図 3】

会員氏名	会員 ID 番号	基本認証 パスワード情報	移動体通信端末 呼び出し番号	移動体通信経由情報 パスワード情報
渡辺	NABE	GT104	060211	3023
小林	HIRO	GT110	090320	5066
池田	KICHI	GT112	0702300	4045

【圖 4】



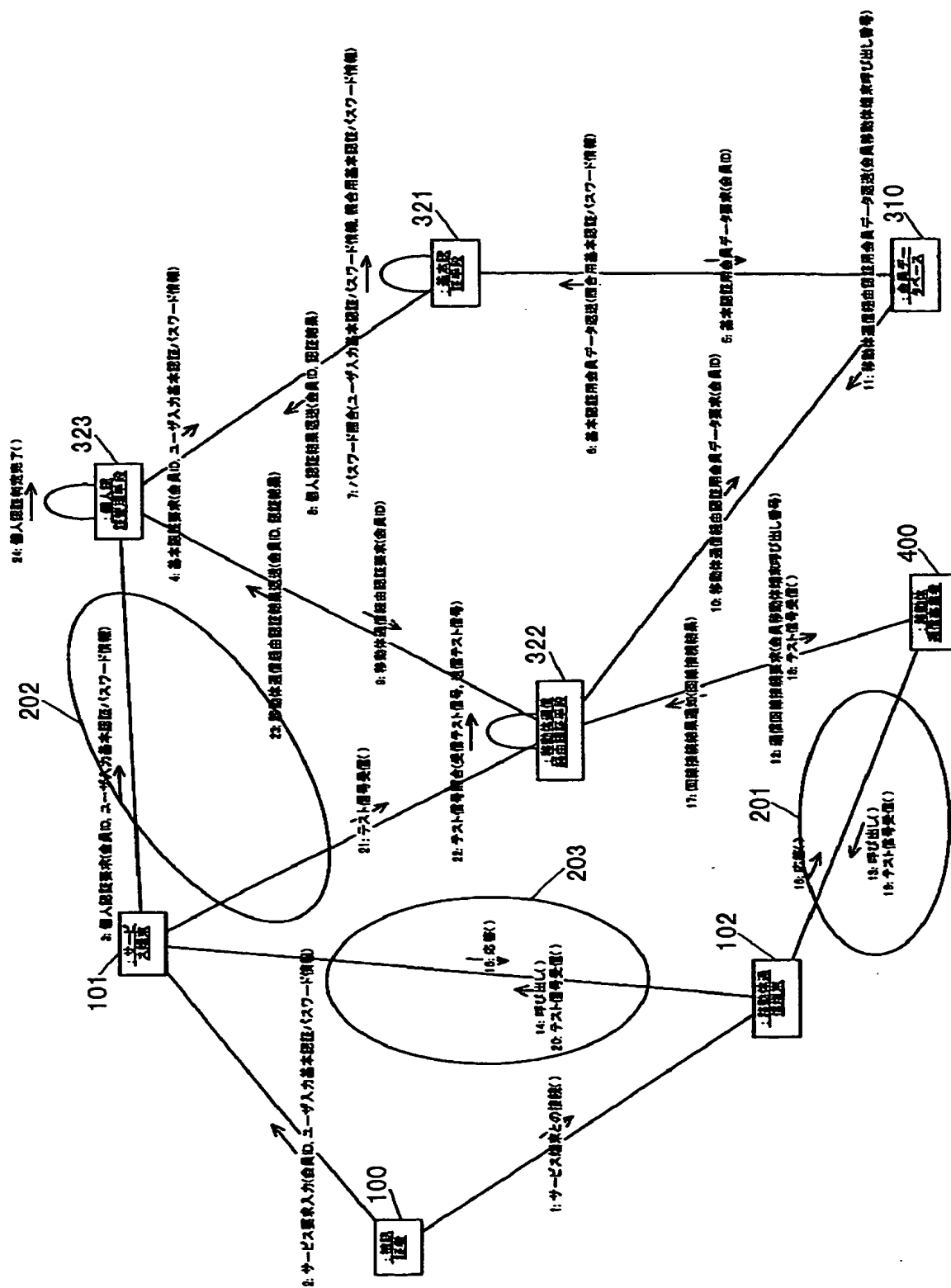
【図 5】



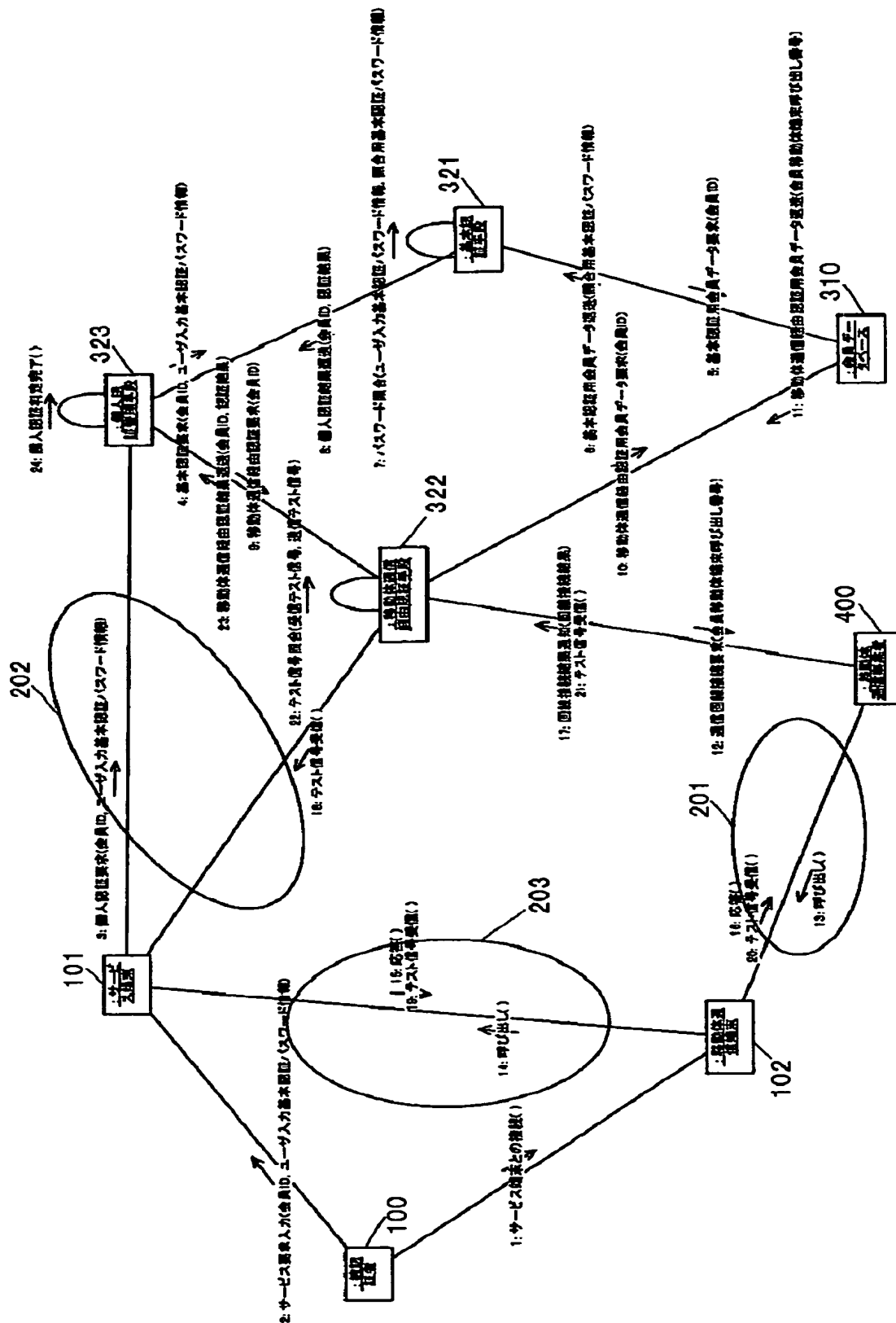
【図 6】

会員 ID 番号	基本認証用 パスワード情報	移動体通信経路認証用 パスワード情報
NABE	GT104	3023
HIRO	GT110	5066
KICHI	GT112	4045

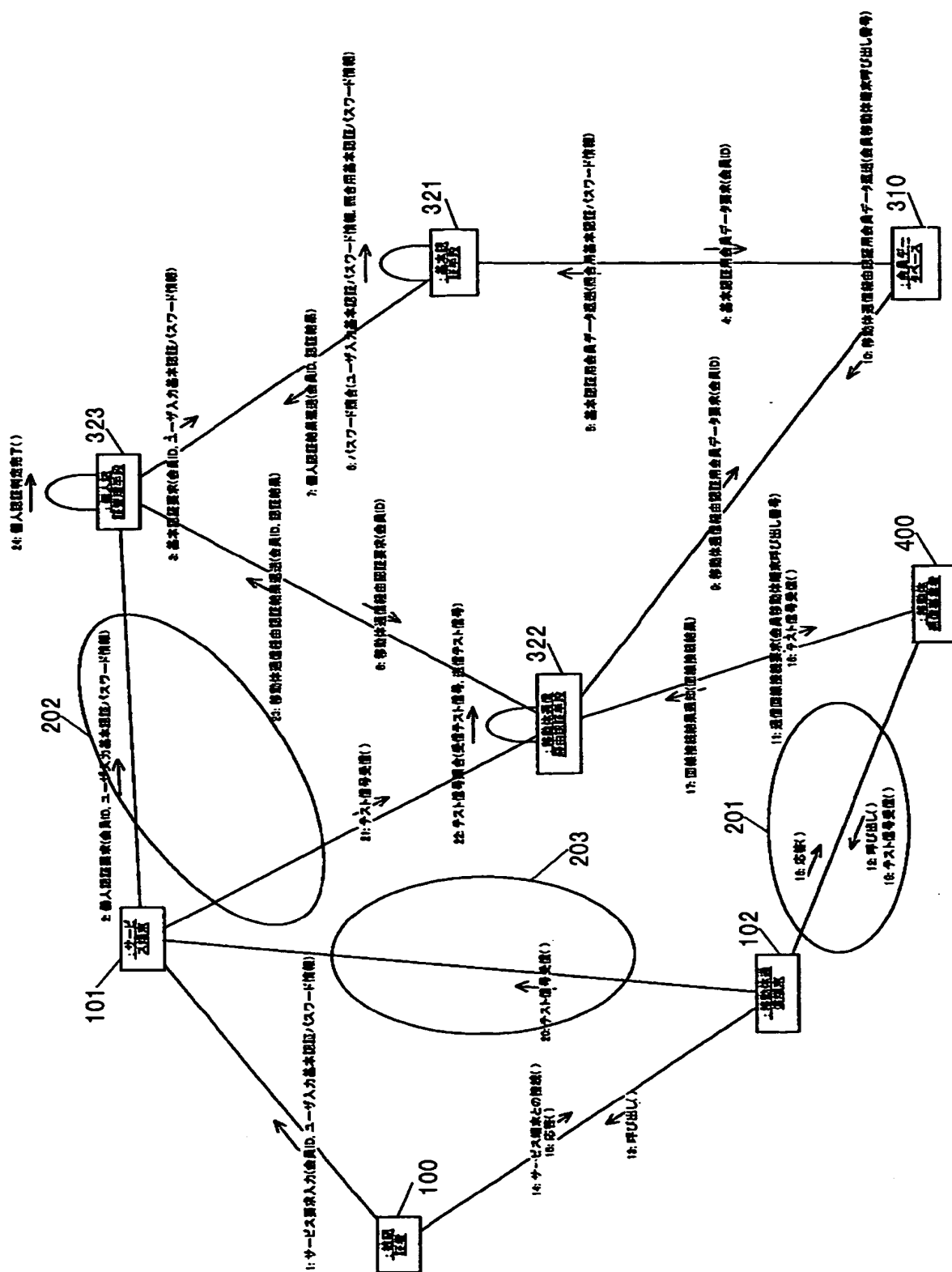
【图 7】



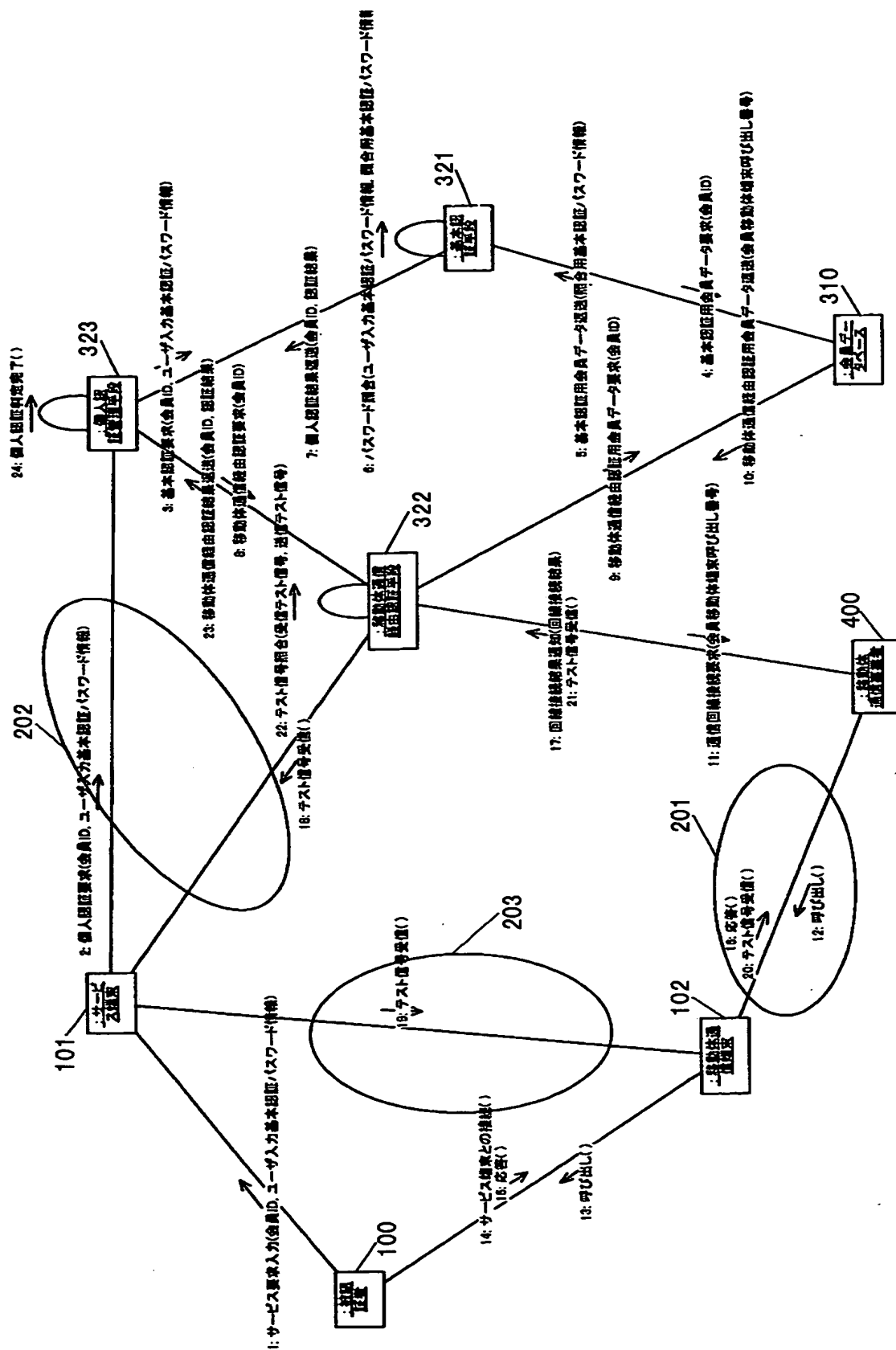
【圖 8】



【図 9】



【図 10】



【書類名】 要約書

【要約】

【課題】 インターネット等を用いてサービスを提供する場合に、過度に複雑化することなくセキュリティを強化する個人認証システムの提供を目的とする。

【解決手段】 サービス提供装置 3 0 0 は、サービス対象者として事前登録されている会員の情報を記憶する会員データベース 3 1 0 と、オープンな情報通信路 2 0 2 を用いて会員であることを認証する基本認証手段 3 2 1 と、会員データベース 3 1 0 に事前に登録した移動体通信端末 1 0 2 を経由した認証を実行する移動体通信経由認証手段 3 2 2 とを備え、被認証者 1 0 側は、サービス提供装置 3 0 0 とオープンな情報通信路 2 0 2 で接続されたサービス端末 1 0 1 と、会員データベース 3 1 0 に登録されている移動体通信端末 1 0 2 を備えており、この構成により、オープンな情報通信路 2 0 2 と移動体通信通信路 2 0 1 の 2 つの通信路で認証を行うことが可能となる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社